



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,273	01/27/2000	Wolfgang Rankl	JEK/Rankl	9676

7590

02/02/2005

J. Ernest Kenney
Bacon & Thomas PLLC
625 Slaters Lane
4th Floor
Alexandria, VA 22314-1176

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 02/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application N .

09/492,273

Applicant(s)

RANKL, WOLFGANG

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 September 2004.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☐ Claim(s) _____ is/are rejected.
7) ☒ Claim(s) 1-9 is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 27 January 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 9/9/04 was received and considered.
2. Claims 1-9 are pending.
3. Applicant appears to have filed an RCE on 9/9/04, however, an RCE is proper only if prosecution is closed (see C.F.R. §1.114). The submission of 9/9/04 will be treated as a reply to non-final Office Action, set forth in C.F.R. §1.111.

Response to Arguments

4. Applicant's arguments filed 9/9/04 have been fully considered but they are not persuasive.
5. Applicant's response (p. 2, ¶2) argues that Schneier does not involve any sort of initialization step. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. The Schneier reference merely discloses method steps. Without recitation in the claims of further method steps that occur either before or after the currently claimed steps, initialization is simply a use. Further, an invention can be initialized many times during its use. Absent further boundaries on the method steps, recitation that initialization is the purpose of the steps does not affect the method steps. See *In re Casey*, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 136

Art Unit: 2134

USPQ 458, 459 (CCPA 1963). Chen is relied upon for teaching that smart cards need to be initialized (col. 4, lines 5-31).

6. Applicant's response (p. 2, ¶2) argues that “no part of the keys are exchanged, in either plain text or encrypted form” in the claimed invention. Claim 1 does not recite the word “key”. Claim 7 recites that the “secret initial value is a key ...”. Schneier discloses the Diffie-Hellman algorithm, where a secret key is generated (both k and k' are secret keys). This limitation is shown in the reference (p. 513, last ¶).

7. Applicant's response (p. 2, ¶2) argues that Chen simply discloses “storage” of the keys on the card, that must be “transferred” and that there is no suggestion in the Chen patent that the storage of keys on the card involves anything other than the usual transfer. However, Schneier teaches that Alice and Bob computed a secret key independently (p. 514) and that public key cryptography allows key exchange if the key cannot be securely transferred (§8.3). Hence, the modification of Schneier to be used with a smart card (Chen) discloses the initialization of keys on a card.

8. Applicant's response (p. 3, ¶1) argues that

“Schneier discloses a data exchange algorithm (the Diffie-Hellman algorithm) that is suitable for exchanging data with an already initialized card (i.e., one that already includes encryption keys), but that is not disclosed as being suitable for card initialization requiring data to be written to the card so that Diffie-Hellman exchanges can subsequently be carried out, and nothing in the Chen patent suggests otherwise. The Schneier article is not concerned with how the secret values used to generate the session keys were established in the first place (the initialization procedure).”

Applicant is directed to the fact that Schneier does not disclose “an already initialized card”. Schneier discloses a protocol whereby a common key can be generated by two entities. Subsequent Diffie-Hellman exchanges are not claimed.

9. Applicant's response (p. 3, ¶2) argues that the Chen patent requires a physically secure location. Schneier teaches the benefit of Diffie-Hellman, which overcomes this limitation. Schneier teaches that a physically secure location is difficult, if impossible, and therefore, public key cryptography is used (of which Diffie-Hellman is the basis). Chen is not relied upon for teaching an algorithm to initialize a chip card – only that it is known to use chip cards with keys stored on them, and that there is a need to initialize the chip cards with the keys.

10. Applicant's response (p. 4, ¶1 – p. 5, last ¶) argues that the combination of Schneier and Chen fails to disclose initialization. Applicant is referred to the preceding response to arguments.

11. Applicant's response (p. 6, ¶1) argues that Barlow teaches away from the claimed invention because Barlow fails to exchange parts of secret values. Claim 8 recites that the key generated in the processing station and the chip card is used in a personalizing step for encrypting and decrypting further secret keys, which are transmitted from the processing station to the chip card.” However, Schneier teaches key-encrypting keys (pp. 176-177, §8.3), where a key-encrypting key exists in a device, such as a smart card and is used to encrypt and decrypt data keys, which are exchanged more often. Barlow is cited for teaching that to support multiple applications, multiple keys (data keys) must be provided to the card (col. 4, lines 34-49). Therefore, Barlow does not teach away from the claimed invention.

12. Applicant's response (p. 6, ¶3-4) argues that Gasser, in combination with Schneier, Chen and Barlow fails to disclose a card “initialization step”. Applicant is directed to the preceding response. Further, it is noted that Gasser is cited for teaching the removal of keys after use. On

Art Unit: 2134

p. 6, 4 of applicant's response, applicant states that the Gasser patent teaches "the secret values used in the public/private session key generating process may be transferred to the chipcard by a secret value generated in the manner claimed, using parts of two picnics in the manner claimed". While the Examiner assumes applicant means "two secret values", it is unclear what part of the Gasser patent applicant is referencing. Further, it is noted that Gasser is not relied upon for teaching the initialization step, but rather the removal of keys after use.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1, 3-5 & 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Applied Cryptography, Second Edition by Schneier in view of U.S. Patent 5,602,918 to Chen et al. (Chen).

Regarding claims 1 & 3-5, Schneier teaches generating first values/(x, X) for determining the secret initial value/k (page 513, step 1), transmitting parts of the first values/X (page 513, step 1), generating second values/(y, Y) for determining the secret initial value/k' and transmitting parts of the second values/Y (page 513, step 2), determining the secret initial value/k from at least parts of the first values/x and the transmitted parts of the second values/Y (page 513, step 3) and determining the secret initial value/k' from at least parts of the second values/y and the transmitted parts of the first values/X. Schneier lacks inserting a chip card into a

Art Unit: 2134

processing station and lacks initializing the chip card by having the processing station perform steps 1 and 3 in the Schneier reference and the chip card perform steps 2 and 4 in the Schneier reference. Schneier only teaches a mathematical protocol, lacking implementation details, and hence lacks inserting a chip card into a processing station and initializing the chip card.

However, Chen teaches that to initialize a smart card with a master key, the card/chip card is inserted into an initialization terminal/processing station and the key is transferred, preferably securely (col. 4, lines 5-31). The protocol taught by Schneier is beneficial over a standard key transfer, because no one listening to the exchanges can recover the key value (Schneier, page 513). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply the protocol of Schneier to the card initialization terminal, as taught by Chen (col. 4, lines 5-31). One of ordinary skill in the art would have been motivated to perform such a modification to initialize a smart card with a master key, as taught by Chen (col. 4, lines 5-31) using a method to enhance the security of initialization, as taught by Schneier (pages 513-514).

Regarding claim 7, Schneier lacks explicitly disclose encrypting and decrypting data with the key. However, the examiner takes Official Notice that using a secret key for encryption is old and well established in the art of cryptography as a method of protecting data. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the secret initial value for encrypting and decrypting data. One of ordinary skill in the art would have been motivated to perform such a modification to protect data from eavesdroppers. This advantage is well known to those skilled in the art.

Art Unit: 2134

15. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Chen, as applied to claim 1 above, and further in view of "Cryptographic Identification Methods for Smart Cards in the Process of Standardization" by Hans-Peter Königs in further view of Handbook of Applied Cryptography by Menezes. Schneier discloses a system, as modified above, but lacks using an individual identifier to generate the initial value for the card. Königs teaches that one can greatly simplify the problem of key management and make an explicit public key unnecessary by deducing a verification key from an identification word/individual identifier (see page 46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Schneier's system to use identification information as the basis for a key. One of ordinary skill in the art would have been motivated to perform such a modification to simplify key management, as taught by Königs (see page 46). Schneier, as modified above, lacks the identification information being a serial number. However, Menezes teaches that sequence numbers can be used to identify entities, often in key establishment protocols (see §10.3.1 & §10.12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the serial number of the smart card for identification, and hence as the basis for the key. One of ordinary skill in the art would have been motivated to perform such a modification to provide uniqueness, as taught by Menezes (see §10.3.1 & §10.12).

16. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Chen, as applied to claim 1 above, and further in view of U.S. Patent 5,452,358 to Normile et al. (Normile). Schneier, as applied to claim 1, does not disclose using the secret initial value as

Art Unit: 2134

the start value for generating random numbers. However, Normile teaches that a secret key can be used as a seed value for generating random numbers, which can then be used to encrypt data (col. 4, lines 9-20). Further, Schneier teaches that good keys are random strings, i.e. a key used for encryption should be, at least to some degree, random (pages 173-174). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the secret initial value as a start value for generating random numbers. One of ordinary skill in the art would have been motivated to perform such a modification to add randomness to the keys used for encryption, as taught by Schneier (pages 173-174) and Normile (col. 4, lines 9-20).

17. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Chen, as applied to claim 1 above, in further view of U.S. Patent 6,038,551 to Barlow et al. (Barlow). Schneier's system, as modified above, lacks transmission of additional keys to the card. Schneier does however teach that keys also need to be cryptographically protected during transport and that it is common to encrypt data keys (keys for encrypting data) with key encrypting keys for transfer (page 176-177, §8.3). However, Barlow teaches that to support multiple applications, the card must enable a user to transport keys from one application to another (see col. 4, lines 34-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Schneier's system to allow multiple keys to be transported through the medium secured by the algorithm (as taught by Schneier). One of ordinary skill in the art would have been motivated to perform such a modification to support multiple applications, as taught by Barlow (see col. 4, lines 34-49).

Art Unit: 2134

18. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Chen in view of Barlow, as applied to claim 8 above, and further in view of U.S. Patent 5,224,163 to Gasser et al. (Gasser). Schneier's system, as modified above, lacks removal of the original session key after the receipt of personalization information. Gasser teaches that removing a key after it's use in an authorization system ensures security even if one of the participants is compromised thereafter (see col. 15, lines 51-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to remove the session key from Schneier's system, as modified above, after the initial transaction was complete. One of ordinary skill in the art would have been motivated to perform such a modification to prevent compromise of both the card and the apparatus if either was compromised, as taught by Gasser (see col. 15, lines 51-65).

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2134

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:


(703)746-7239 (for formal communications intended for entry)

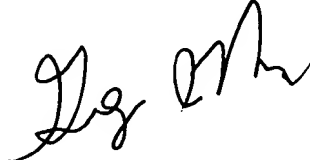
Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


January 24, 2005
MJS


GREGORY MORSE
PATENT EXAMINER
CENTER 2100